Ref. 4

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平2－204768

⑤1Int.Cl.⁵	識別記号	庁内整理番号	⑬公開　平成2年(1990)8月14日
G 09 C 1/00		7368－5B	
H 04 L 9/00		6945－5K　H 04 L 9/00	

審査請求　未請求　請求項の数 3　（全11頁）

⑤4発明の名称　メッセージ変換方法

⑳特　願　平1－24723
㉒出　願　平1(1989)2月2日

⑦2発明者　川村　信一　神奈川県川崎市幸区小向東芝町1　株式会社東芝総合研究所内
⑦1出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地
⑦4代理人　弁理士　須山　佐一

明　細　書

1．発明の名称

メッセージ変換方法

2．特許請求の範囲

（1）メッセージブロックCを他のメッセージブロックMに変換するメッセージ変換方法であって、

秘密鍵n、dを有している第1の装置がm個の乱数R_i（i＝1、…、m）を生成するとともに、この乱数R_iを用いて秘密鍵dからd´を生成する過程と、

d´およびnが前記第1の装置から第2の装置に転送される過程と、

前記第2の装置がメッセージブロックCから

$M´ = C^{d´} \bmod n$

を算出する過程と、

前記第2の装置がM´を算出しているのと並行して前記第1の装置は乱数R_iとnからXを算出する過程と、

M´が前記第2の装置から前記第1の装置に転送される過程と、

前記第1の装置が

$M = M´ \cdot X \bmod n$

によりメッセージブロックMを算出する過程と、

を具備することを特徴とするメッセージ変換方法。

（2）メッセージブロックCを他のメッセージブロックMに変換するメッセージ変換方法であって、

秘密鍵n、dを有している第1の装置がm個の乱数R_i（i＝1、…、m）を生成するとともに、この乱数R_iを用いて秘密鍵dからd´を生成する過程と、

d´およびnが前記第1の装置から第2の装置に転送される過程と、

前記第2の装置がメッセージブロックCから

$M´ = C^{d´} \bmod n$

を算出する過程と、

前記第2の装置がM´を算出しているのと並行して前記第1の装置は乱数R_iとnからX^{-1}を算出する過程と、

M´が前記第2の装置から前記第1の装置に転

送される過程と、

前記第１の装置が

$M = M' \cdot X^{-1} \mod n$

によりメッセージブロックＭを算出する過程と、

を具備することを特徴とするメッセージ変換方法。

（３）メッセージブロックＣを他のメッセージブロックＭに変換するメッセージ変換方法であって、

秘密鍵ｎ、ｄを有している第１の装置がｍ個の乱数R_i（ｉ＝１、…、ｎ）を生成するとともに、この乱数R_iを用いて秘密鍵ｄからｄ′を生成する過程と、

ｄ′およびｎが前記第１の装置から第２の装置に転送される過程と、

前記第２の装置がメッセージブロックＣから

$M' = C^{d'} \mod n$

を算出する過程と、

前記第２の装置がＭ′を算出しているのと並行して前記第１の装置は乱数R_iとｎからＸおよびX^{-1}を算出する過程と、

Ｍ′が前記第２の装置から前記第１の装置に転送される過程と、

前記第１の装置が

Ｍ′，Ｘ，X^{-1}をもちいてメッセージブロックＭを算出する過程と、

を具備することを特徴とするメッセージ変換方法。

３．発明の詳細な説明

［発明の目的］

（産業上の利用分野）

本発明は、暗号を利用するデータ通信等に適用可能なメッセージ変換方法に関する。

（従来の技術）

暗号が提供するセキュリティ・サービスを利用する場合、鍵情報をいかに安全に利用者に配送するか、または鍵情報をどのように保管するかは重要な問題である。

1978年にRivest等によって提案された公開鍵暗号RSA（R.L.Rivest.A.Shamir and L.Adlman: "A method of obtaining digital signatures and cryptosysytems".Coms.of ACM.pp.120-126）はこのような鍵配送問題のかなりの部分を解決できる暗号方式として注目される。RSA暗号は本発明の基盤をなすので、ここで詳しく説明する。

鍵生成

まず、任意の相異なる大きな素数ｐとｑを生成する。生成したｐとｑの積としてｎ＝ｐ・ｑを作る。また、ｐ、ｑよりＬ＝λ（ｎ）＝ＬＣＭ（ｐ-１、ｑ-１）を求める。ここでλはカーマイケル関数を表し、ＬＣＭ（ｐ-１、ｑ-１）はｐ－１、ｑ－１の間の最小公倍数を表す。次にＬと互いに素な適当な整数ｅを選び（３≦ｅ≦Ｌ－１）、法Ｌの下でのｅの乗法逆元ｄを求める。

$e \cdot d \equiv 1 \mod L$　　（１）

このようにして生成された（ｅ、ｎ）が暗号化の鍵であり、復号化は（ｄ、ｎ）を用いて行うことができる。

暗号化と復号化

平文Ｍと暗号Ｃは共にｎ未満の整数である。暗号化は次のようにして行う。

$C = M^e \mod n$　　（２）

また、ＣからＭは次のようにして求められる。

$M = C^d \mod n$　　（３）

この復号化の変換は、受信者の秘密情報であるｐ、ｑを利用すると高速化することができる。その方法についてはJ.J.Quisquater等による文献"Fast decipherment algorithm for RSA public-key cryptosystem".Electron.Lett.,18,21,pp.905-907(Oct.1982)に詳しく述べられている。

式（３）の値を計算するのに法ｎの下で直接求めるのではなく、まず、法ｐとｑの下で計算を進めておき、得られた結果から中国剰余定理を利用して平文を求めるのである。（中国剰余定理については、たとえば池野・小山著「現代暗号理論」電子通信学会編（p19）を参照。）

この方法を具体的に説明するために、C_1、C_2、d_1、d_2、m_1、m_2を次のように定義する。

$C_1 = C \mod p$、 $C_2 = C \mod q$ (4)

$d_1 = d \mod (p-1)$、 $d_2 = d \mod (q-1)$ (5)

$m_1 = M \mod p$、 $m_2 = M \mod q$ (6)

この時、次式が成立する。

$m_1 = C_1^{d1} \mod p$ (7)

$m_2 = C_2^{d2} \mod q$ (8)

これより平文Mは次の連立合同式の根として求められる。

$M \equiv m_1 \pmod p$ (9)

$M \equiv m_2 \pmod q$ (10)

RSA暗号は以上のような手続きで実現されるが、ここでのこの暗号の要点を整理すると、

A．各人ごと異なる公開鍵はe、nはリストのような形で公開されており、だれでもアクセスできる。

B．秘密鍵d、p、q、λ(n)は個人の秘密であり、他人に知られないように十分注意する必要がある。

C．暗号化機能のほかに署名機能がある。

D．RSA暗号の安全性を保障するためには秘密鍵p、qの桁数を各々十進百桁程度の大きさに選ぶ必要がある。nはこの場合、十進二百桁程度の数になり、RSAの暗号化・復号化変換は膨大な処理量の計算となる。

多くの人が加入するネットワークでRSA暗号の利点を最大限に引出せる運用法としては、各人に個別に鍵を発行して、可搬の記憶媒体にその鍵を記憶させ、それを各自が持ち歩くのがよい。この時、上記Bに述べた点は運用上非常に重要である。Bの条件を満足させることのできる個人の秘密鍵の格納媒体としては、ICカードが携帯性のある個人対応の計算装置および記憶装置として最も好適である。しかしながら、実際にICカードを利用したRSA暗号のシステムを構築しようとすると次のような二つの問題が生ずる。

ICカードに鍵を格納した場合、上記Bの要求から、理想的にはICカード内でRSAの復号変換および署名作成を行うのが良い。ICカードにはパスワード照合によるアクセス制御機能があるので、ICカード内で変換を行えばd、p、q、λ(n)がICカード外に洩れる心配はなくなるからである。しかしながら、現状では上記Dに述べたことおよびICカードの計算力不足が理由でRSA暗号の変換をICカードで行った場合に、実用上十分な処理速度を達成することができない。これは前記Quisquater等の高速化手法を用いても同様である。また、RSA専用の高速演算LSIをICカードに実装することも考えられるが、カードコストの増大は避けられない。

一方、ICカードを単にアクセス制御機能のある、鍵メモリとして利用することは容易である。手間のかかる暗号変換は計算能力の高いICカード外の装置、たとえば端末装置に行わせることによって実用的な処理速度を達成可能である。しかし、この場合にはdを端末装置に渡すことになるので、端末装置の設計および維持管理に十分な注意を怠ると、端末装置経由でdが他人に洩れる恐れがある。また、偽の端末装置によって知らぬ間にdを盗まれるかもしれない。

このような二つの問題点を解決するために、最近、端末装置には秘密鍵dに関する情報をもらさずに、端末装置の計算力のみを借りてICカードが効率よくRSAの暗号変換を行える手段が提案された。これを提案者らにならって以下「依頼計算法」と呼ぶことにする。依頼計算そのものはひろい概念であるが、これをRSA暗号の変換に応用する手法で本発明と関連が深い方式は文献「安全な計算依頼法について」(加藤、松本、今井、1988年 暗号と情報セキュリティ シンポジウム資料F-3、1988、2月)に示されている。以下、その方式を説明するとともに、第7図にその手順を概念的に示す。

準備として、まず次の関係式を満たすr_p、

r_q、Rを求める。

$$r_p = R^{-1} \bmod (p-1) \quad (11)$$

$$r_q = R^{-1} \bmod (q-1) \quad (12)$$

ただし、$x(r) = \ell(r) + w(r) - 2$と定義するとき、$r_p$、$r_q$は、

$$x(r_p) + x(r_q) \quad (13)$$

が小さい数であるように選ばれる。なお、$\ell(r)$はrのビット長、$w(r)$はrのハミング重みを表わし、$x(r)$はrを指数とするべき乗剰余計算に要する剰余乗算の回数を表わしている。

また、

$$w_p = q(q^{-1} \bmod p) \bmod n,$$

$$w_q = p(p^{-1} \bmod q) \bmod n \quad (14)$$

も計算しておく。ICカード内にはr_p、r_q、R、d、p、q、$\lambda(n)$、n、w_p、w_qが記憶されている。

次にICカードはdの代わりに、

$$d' = d \cdot R \bmod \lambda(n) \quad (15)$$

を用いて、端末装置に対してCをd'で変換したM'の計算を依頼する（ステップ701、702）。ただし、

$$M' = C^{d'} \bmod n. \quad (16)$$

端末装置は計算したM'をICカードに送り返す（ステップ703）。ICカードはこれを次式によって変換し、平文Mを得る（ステップ704）。

$$M = \{(M' \bmod p)^{r_p} \bmod p\} w_p + (M' \bmod q)^{r_q} \bmod q) w_p\} \bmod n \quad (17)$$

（13）式が小さい値になるようなr_p、r_qを選んでいるので、（17）式に現れるべき乗剰余計算は計算力の比較的小さなICカードでも効率よく計算することができる。また、端末装置に対してはdを直接示すのではなく、（15）式による変換を施したd'を見せるだけなので安全性は高くなる。このように依頼計算によれば、秘密鍵dの機密性を増しつつ端末装置の計算力を借りて効率良く復号変換を行うことができる。

さて、実用的なシステムに上記の依頼計算法を適用した場合を考察してみることにする。（15）式の変換は事前に行うことができるので、復号変換開始以降、実際に行わなければならないのは（16）、（17）式の変換のみである。（17）式の変換の右辺は（16）式で計算されるM'を含んでいるので、（17）式は（16）式の処理が終わってからでないと実行できない。すなわち、復号変換の処理時間は、（16）および（17）式の処理に要する演算時間の和で定まることになる。一方、端末装置が行う（16）式の変換は、たとえば汎用の高性能汎用16ビットマイクロプロセッサである80286で実行してもnが512ビット程度のときには約30秒の処理時間を要する。したがって、外部計算装置をよほど高性能の専用マシンで実現しない限り、ここで説明した依頼計算によって演算時間を十分小さくすることは不可能である。

以上まとめると、まずRSA暗号は計算の手間が大きいので、ICカードのような計算力が比較的小さい装置で実行させようとすると多大な計算時間を要する。また、RSAの計算を高速に行える外部装置を用意して、これを計算させようとすると、復号変換やディジタル署名作成に必要な秘密情報を外部装置に知られてしまい、不正使用される恐れがあった。また「依頼計算」を用いて秘密情報は外部装置にもらすことなく、外部装置の計算力のみを借りて効率よく変換を行う手法が提案されているが、従来、提案されている方法では、確かにICカードが行うべき処理の量は減らすことはできるものの、ICカードが実行する計算と外部装置が行う計算とは同時に並列処理することができず、外部装置が極めて高速な処理を行うのでなければ、その効果は半減してしまう方式であった。

（発明が解決しようとする課題）

以上の問題点に鑑み、本発明の目的は、端末装置の処理とICカードの処理の大部分とを同時に行える方式を提供することによって、依頼計算に要する処理時間を従来方式に比べて大幅に短縮させ、さらに、端末装置およびICカードの処理速度を過剰に速くする必要をなくし、端末装置のコストおよびICカードのコストを押えることにある。

［発明の構成］

（課題を解決するための手段）

本発明は、メッセージブロックCを他のメッセージブロックMに変換するメッセージ変換方法であって、秘密鍵n、dを有している第1の装置がm個の乱数R_i（i＝1、…、m）を生成するとともに、この乱数R_iを用いて秘密鍵dからd´を生成する過程と、d´およびnが前記第1の装置から第2の装置に転送される過程と、前記第2の装置がメッセージブロックCから

$$M' = C^{d'} \bmod n$$

を算出する過程と、前記第2の装置がM´を算出しているのと並行して前記第1の装置は乱数R_iとnからXを算出する過程と、M´が前記第2の装置から前記第1の装置に転送される過程と、前記第1の装置が

$$M = M' \cdot X \bmod n$$

によりメッセージブロックMを算出する過程と、を具備することを特徴とする。

（作用）

このように構成されたメッセージ変換方法では、まず第2装置が知るのは公知のd´とnとCおよびM´のみであり、特に秘密鍵dを直接知ることができないので、第2の装置にdを持ち逃げするなどという不正な機能を仕組もうとしても不可能となる。また、第1の装置が実行する演算のうち、X_{pl}、X_{ql}またはX_lを求める部分は、第2の装置の演算とは独立に行える。また、乱数r_{pl}、r_{ql}のビット長に制約をつければ、X_{pl}、X_{ql}を計算する演算量も削減できる。

（実施例）

本発明の実施例を以下に述べる。説明の都合上、第1図に示すように計算依頼側をICカード、計算請負側を端末装置として以下説明するが、依頼側と請負側は独立な装置、ソフトなど、この節での説明を越えない範囲で任意である。また、実施例の説明では暗号文Cを平文Mに戻す処理に関する依頼計算として説明するが、同一の変換で実現されるディジタル署名の作成にも本発明は適用可能である。

第2図はこのメッセージ変換方法に用いられる端末装置2の斜視図である。

同図に示されるようにこの端末装置2は本体1、ディスプレイ3、キーボード5、リードライタ7を有している。そしてリードライタ7にICカード9が挿入され、本体1にフロッピィーディスク11が挿入される。

第3図はICカード9の構成を示すブロック図であり、このICカード9はI／Oコンタクト13、CPU15、データメモリ17、プログラムメモリ19とを有する。

第4図は本体1の構成を示すブロック図であり、この本体1はディスプレイコントローラ21、中央処理装置23、メインメモリ25、第1通信ポート27、第2通信ポート29、フロッピィーディスクドライバ31、キーボード（I／O）33とを有し、これらが内部データバス35で接続される。ディスプレイコントローラ21はディスプレイ3を制御する。中央処理装置23はこの端末装置2全体を制御する。メインメモリ25はフロッピーディスク11に記憶されているデータの蓄積等を行う。

第1通信ポート27は通信回線12に接続され、この通信回線12は他の端末装置2と接続されている。第2通信ポート29はリードライタ7に接続されている。フロッピィーディスクドライバ31はフロッピィーディスク11を駆動する。キーボード（I／O）33はキーボード5と接続されている。

次にこの端末装置2とICカード9を用いてメッセージ変換方法について説明する。

まず、準備として（11）、（12）によく似た式（18）、（19）を満たす適当な乱数の組r_p、r_q、Rを求める。

$$r_p = R \bmod (p-1) \quad (18)$$

$$r_q = R \bmod (q-1) \quad (19)$$

この時、従来技術と同様に、

$$x(r_p) + x(r_q) \quad (20)$$

が比較的小さい数であるという制約を課す。

（18）、（19）式の連立方程式は、r_p、r_q

を適当に定めてその後に求めるもので、解の存在条件および解法は、たとえば、高木貞治：“初等整数論講義”，共立出版，pp.31-35に示されている。この連立方程式の解はL－LCM（p-1、q-1）を法として唯一定まる。また、必要に応じて、

$$w_p = q\,(q^{-1} \bmod p) \bmod n,$$

$$w_q = p\,(p^{-1} \bmod q) \bmod n \qquad (21)$$

も計算しておく。後に述べるようにw_p、w_qは必ず用意しなければならない定数ではない。本実施例においてはICカード内にはr_p、r_q、d、p、q、λ（n）、n、d′、w_p、w_qが記憶されている。

本発明の最も単純で、かつ最もその効果が顕著な実施例として、dからd′を求める変換を、

$$d' = (d - R) \bmod \lambda(n) \qquad (22)$$

と定義する場合を説明する。

端末装置2の処理フローを示したのが第5図である。

まず、ユーザは端末装置2に向かうとともに、自分のICカード9を端末装置2に接続されたICカード9のリーダ・ライタ7に挿入する（ステップ501）。

そして、端末装置2の適当なキーを叩き使用開始を端末装置2に知らせる。この時、同時にリーダ・ライタ7を介してICカード9にクロックおよび電源が供給され、適当な初期化（ステップ502）の後にICカード9は通信待ち状態となる。端末装置2はICカード9のユーザ確認を行うために、ユーザに対してパスワードの入力を指示する（ステップ503）。

パスワードが入力されない場合（スッテプ504），時間をチェックし（ステップ505），時間切れの場合はタイムアウトとなり，そうでない場合はステップ503に戻る。パスワードが入力されるとICカード9にパスワードが転送され（ステップ506），このパスワードはICカード9内に記憶されている登録パスワードと比較され、照合結果が端末装置2に転送される（ステップ507）。照合結果が一致していれば（ステップ508）、ICカード9は使用可能状態となるが、一致しない場合にはICカードは使用不能である。ユーザからのコマンド入力があると（ステップ509）、終了コマンドであるかないかが判断され（ステップ510），コマンドサブルーチンの実行が行われる（ステップ511）。

次にコマンドサブルーチンの実行について述べる。

これ以降の手順は、第1図に示されている。

端末装置2はこの暗号文Cをまず ICカード9宛てに伝送し（ステップ101）、同時にICカード9のメモリに書込まれているd′とnを読み出す（ステップ102）。端末装置2はこの二つの情報を用いて暗号文Cから、M′を次式に従って計算する（ステップ103）。

$$M' = C^{d'} \bmod n \qquad (23)$$

端末装置2は計算したM′をICカード9に送る（ステップ105）。

一方、ICカード9は端末装置2の計算と並行して、（24）～（26）式に従って定数Xを求める（ステップ104）。

$$X_p = (C \bmod p)^{r_p} \bmod p \qquad (24)$$

$$X_q = (C \bmod q)^{r_q} \bmod q \qquad (25)$$

を計算し、次式によってXを求める。

$$X = \{(X_p)^{r_p} \bmod p)\, w_p + (X_q)^{r_q} \bmod q)\, w_q\} \bmod n \qquad (26)$$

ここで、（24）～（26）式について補足説明しておく。

（24）、（25）式はXに関する連立方程式と見ることができるが、中国剰余定理よりこの2式を満たすXは一意に定まる。そして、その一解法が（26）式の右辺である。ここでは先に計算したw_p、w_qなる二つの補助変数を用いてXを導出している。

しかし、（24）、（25）を満たすXの導出法はこれに限らない。たとえば前出のJ.J.Quisquater等による文献“Fast decipherment algorithm for RSA public-key cryptosystem”.Electron.Lett..18.21.pp.905-907(Oct.1982)にはこの種の連立方程式の別な解法が示されている。

したがって、（26）式によるXの導出および補

助変数w_p、w_qの使用は本質的ではなく、（24）、（25）を同時に満たすXを求めることのみが本質である。それゆえ、この実施例が本発明を実際に応用する場合のXの求め方を限定するものではない。

さて、ICカード9が本来求めたかった平文Mは暗号文Cを、

$$M = C^d \bmod n \qquad (27)$$

と変換して得られるが、このMは端末装置2が計算したM′とICカード9が計算したXとから次式によって求められる（ステップ106）。

$$M = (M' \cdot X) \bmod n \qquad (28)$$

この計算は、この例ではICカード9の内部で行われる。ICカードは得られたMを復号結果として端末装置2に伝送する（ステップ107）。

端末装置2はこれをディスプレイに表示するとともに、ユーザからの指示で補助記憶装置に書込んで一連の復号化手続きを終了し、ユーザはリーダ・ライタ7からICカード9を抜き取り、作業を終了する。

ここで、本実施例において手続きの過程で知ることのできる端末装置2はMとM′からXを容易に求められるので、（28）式の計算はICカード9で行わないで端末装置2で行っても良いことを注意しておく。そのような手順のときには端末装置2がICカード9にM′を伝送するのではなく、ICカード9が端末装置2に対してXを伝送することになる。

以上の手続きの中で、（28）式でMが正しく計算できることは、以下のように説明される。

まず、（24）～（26）より、

$$X = C^R \bmod n \qquad (29)$$

である。これは（従来の技術）でふれた中国剰余定理より明らかである。

一方、

$$\begin{aligned} M' &= C^{d} \bmod n \\ &= C^{(d-R) \bmod \lambda(n)} \bmod n \\ &= C^{d-R} \bmod n \\ &= C^{d} C^{-R} \bmod n \end{aligned} \qquad (30)$$

（29）、（30）式より、

$$\begin{aligned} (M' \cdot X) \bmod n &= (C^{d} C^{-R} \cdot C^{R}) \bmod n \\ &= C^{d} \bmod n \\ &= M \end{aligned} \qquad (31)$$

これで（28）式が成立つことが示された。

次に、計算の手間について考察する。まず、（18）～（22）までの計算は変換を開始する以前に準備しておくことができる。暗号文Cが与えられ、初めて実行可能な部分の計算のみを考慮すればよい。Cが与えられて以降実行する手続きとして、

①ICカード9が行う、（24）～（26）式によってXを求めること、

②端末装置2が行う（23）式の計算、

③ICカード9が行う（28）式の計算、

がある。このうち最も演算手段が多いのは②の端末装置2の計算である。具体的にはこの値は$\lambda(d')$で表されるが、nが512ビットの場合には、これは最悪で1024回程度の512ビットのべき乗剰余計算になる。次に、演算手数が多いのは①である。①のうち支配的なのは（24）、（25）の計算であり、それは$x(r_p)+x(r_q)$回の256ビットのべき乗剰余演算である。r_p、r_qを予め小さく選んでおくことにより、この演算量が押えられる。また、ICカードが行う③の演算は512ビットの剰余乗算1回である。全体として①②の演算が支配的である。さらに、本発明において特に注意すべきは、①の手続きと②の手続きが独立であり、同時に並列処理できるということである。たとえば、②の処理が汎用パソコンで30秒かかるとするとき、r_p、r_qを適当なビット長に定めてICカードでの①の演算時間を30秒程度にすれば、復号に要する総演算時間はほぼ30秒となる。①～③の処理に要する時間を各々T1、T2、T3で表すと、一般に総演算時間Tは、

$$\begin{aligned} T &= Max(T1, T2) + T3 \\ &\fallingdotseq Max(T1, T2) \end{aligned} \qquad (32)$$

で表せることになる。ただし、Max（A、B）はA、Bのうち、大きい方を取る関数である。

第1の実施例において、M′と（Xp、Xq）の組、もしくはこの組と等価な値を用いてMを導

く手順はここに示した方法に限らない。別の導出法を次に示す。

Mより次の2式から、

$$M'_p = M' \bmod p \quad (33)$$

$$M'_q = M' \bmod q \quad (34)$$

M'_p、M'_qを求めて、

$$M_p = M'_p \cdot X_p \bmod p \quad (35)$$

$$M_q = M'_q \cdot X_q \bmod q \quad (36)$$

を得る。(35)、(36)を連立させれば所望のMが得られる。

本発明の第2の実施例として第6図に従って、dからd'を求める変換を、

$$d' = (d + R) \bmod \lambda(n) \quad (37)$$

と定義する場合を説明する。これ以降の実施例の説明では端末装置2の起動や、ICカード9の初期化に関する説明は省略し、演算の手続きのみ順序を追って説明する。Rは第1の実施例で用いたものと同じとする。第1の実施例同様に、端末装置2は外部から与えられた暗号文CをICカードに伝送し(ステップ601)、ICカードからd'、nを受取る(ステップ602)。端末装置2は第1の実施例同様、次式で与えられる、M'を計算する(ステップ603)。

$$M' = C^{d'} \bmod n \quad (38)$$

端末装置2は計算したM'をICカード9に送り返す(ステップ607)。

一方、ICカード9は、

$$X_p = (C \bmod p)^{rp} \bmod p \quad (39)$$

$$X_q = (C \bmod q)^{rq} \bmod q \quad (40)$$

を計算し(ステップ604)、次式によってXを求める(ステップ605)。

$$X = \{(X_p)^{rp} \bmod p)\, w_p + (X_q)^{rq} \bmod q)\, w_q\} \bmod n \quad (41)$$

さらに、方程式

$$X^{-1} \cdot X = 1 \bmod n \quad (42)$$

を解いてX^{-1}を求める(ステップ606)。この解法は拡張ユークリッドの互除法と呼ばれ、詳細は、たとえば前出の「現代暗号理論」を参照。

さて、ICカードが本来求めたかった値、Mは

$$M = C^d \bmod n \quad (43)$$

であるが、これは端末装置2が計算したM'とICカードが計算したX^{-1}とから次式によって求められる(ステップ608)。

$$M = (M' \cdot X^{-1}) \bmod n \quad (44)$$

ICカード9は得られた結果を端末装置2に伝送し処理を終了する(ステップ609)。

(44)式でMが正しく計算できることは以下のように説明される。

まず、(35)～(38)および中国剰余定理より、

$$X^{-1} = C^{-R} \bmod n \quad (45)$$

である。

一方、

$$\begin{aligned} M' &= C^{d'} \bmod n \\ &= C^{(d+R) \bmod \lambda(n)} \bmod n \\ &= C^{d+R} \bmod n \\ &= C^d C^R \bmod n \end{aligned} \quad (46)$$

(29)、(30)式より、

$$\begin{aligned} (M' \cdot X^{-1}) \bmod n &= (C^d C^R \cdot C^{-R}) \bmod n \\ &= C^d \bmod n \\ &= M \end{aligned} \quad (47)$$

これで(28)式が成立つことが示された。

第2の実施例において、M'と(X_p、X_q)組もしくはこの組と等価な値を用いてMを導く手順はここに示した方法に限らない。

たとえば、予めC^{-1}を拡張ユークリッドの互除法により計算しておけば、

$$X_p^{-1} = (C^{-1} \bmod p)^{rp} \bmod p \quad (48)$$

$$X_q^{-1} = (C^{-1} \bmod q)^{rq} \bmod q \quad (49)$$

が計算でき、これを用いてX^{-1}を計算できる。Mの導出は(40)式同様に行えば良い。

また、Mより次の2式から、

$$M'_p = M' \bmod p \quad (50)$$

$$M'_q = M' \bmod q \quad (51)$$

M'_p、M'_qを求めて、

$$M_p = M'_p \cdot X_p^{-1} \bmod p \quad (52)$$

$$M_q = M'_q \cdot X_q^{-1} \bmod q \quad (53)$$

を得る。(48)、(49)を連立させれば所望のMが得られる。第2の実施例の効果も第1の実施例の説明の最後に述べたことと同様である。

第3の実施例として、より一般化された方式を

説明する。第１、第２の実施例では各々カーマイケル関数λ(n)を法とする代数系の上で唯一の乱数Ｒを用いていた。第３の実施例ではｍ個の乱数Ｒｉ（ｉ=1、…、ｍ;ｍ≧1）を用いた一般形について説明する。まず、各乱数Ｒｉは、各々次の方程式を満たしているとする。

$$R_i \bmod p = r_{ip} \quad (54)$$

$$R_i \bmod q = r_{iq} \quad (55)$$

なお、第１の実施例同様、

$$x(r_{ip}) + x(r_{iq}) \quad (56)$$

の大きさに適当な制約を付けるものとする。（54）～（56）式よりわかるように、先にr_{ip}、r_{iq}を定めて、それからＲｉを求める。

このようにして求めたＲｉを用いて次のようなｘからｙへの変換ｆｉをそれぞれ定める。

$$y = f_i(R_i, x) \quad (57)$$

このように定めたｍ個の変換を合成した変換を用いてｄをｄ′に変換する。

$$d' = f_m(R_m, \cdots, f_2(R_2, f_1(R_1, d))\cdots) \quad (58)$$

ｆｉの具体的定義としては次の３種類を用いることができる。

$$y = x \cdot (R_i^{-1}) \bmod \lambda(n) \quad (59)$$

$$y = (x - R_i) \bmod \lambda(n) \quad (60)$$

$$y = (x + R_i) \bmod \lambda(n) \quad (61)$$

（59）式は従来の技術で述べた関数であり、（60）、（61）式はそれぞれ、第１、第２の実施例で示した関数である。これらの任意の組合わせを用いて依頼計算を実現できる。

前の例と同様に、（58）式で求めたｄ′をＩＣカード９は端末装置２に送る。端末装置２は、次式によりＭ′を求める。

$$M' = C^{d'} \bmod n. \quad (62)$$

端末装置２はＭ′をＩＣカード９に送り返し、ＩＣカード９はこれを（58）式の変換手順によって定まるＭ導出の手順に従ってＭ′からＭを求める。前の例同様（60）式、（61）式に対応する変換については、端末装置２での計算と平行して、

$$X^{pi} = (C \bmod p)^{r_{ip}} \bmod p \quad (63)$$

$$X^{qi} = (C \bmod q)^{r_{iq}} \bmod q \quad (64)$$

など、Ｍ′からＭを求める変換に必要な値を計算することができる。本例で具体的にどうしてＭを求めるかは従来技術および第１、第２の実施例を繰返し適用するだけで容易に実現できるので、これ以上の説明は省略することにする。

［発明の効果］

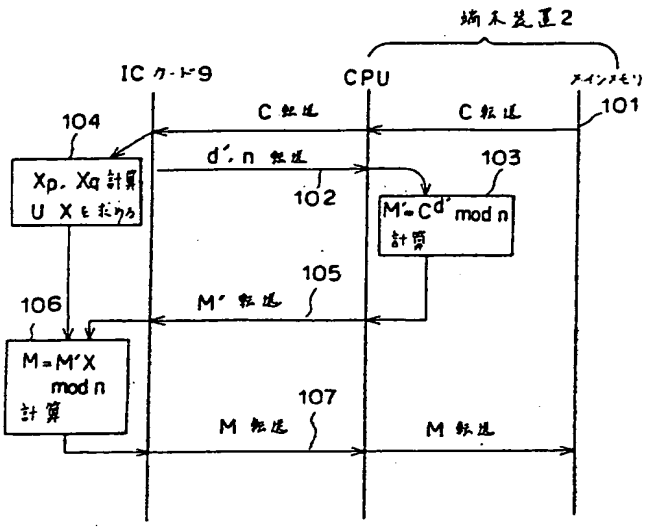
以上説明したように本発明によれば、端末装置の処理とＩＣカードの処理の大部分を同時に行える方式を提供し、依頼計算に要する処理時間を従来方式に比べて大幅に短縮することができる。さらに、本発明によれば端末装置およびＩＣカードの処理速度を過剰に速くする必要がなく、端末装置のコストおよびＩＣカードコストを押えることができる。

４．図面の簡単な説明

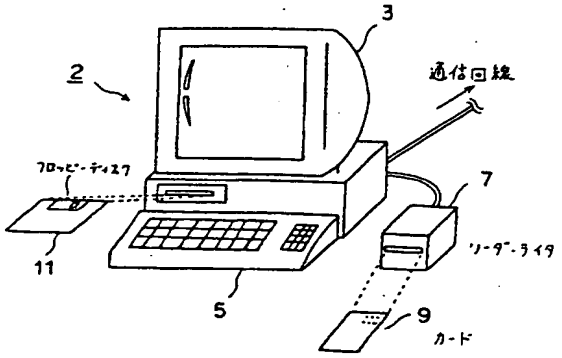
第１図は本発明の実施例に係るメッセージ変換方法の処理フローを示す図、第２図は端末装置２の斜視図、第３図はＩＣカード９の構成を示すブロック図、第４図は端末装置２の構成を示すブロック図、第５図は端末装置２の処理を示すフローチャート、第６図は他の実施例に係るメッセージ変換方法の処理フローを示す図、第７図は従来の処理フローを示す図である。

１……本体
９……ＩＣカード
１１……フロッピィーディク
１５……ＣＰＵ
２３……中央処理装置
２５……メインメモリ

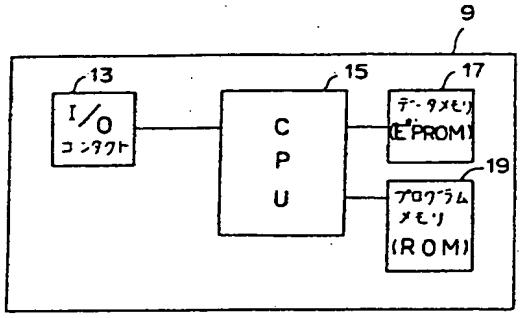
出願人　株式会社　東芝
代理人　弁理士　須　山　佐　一



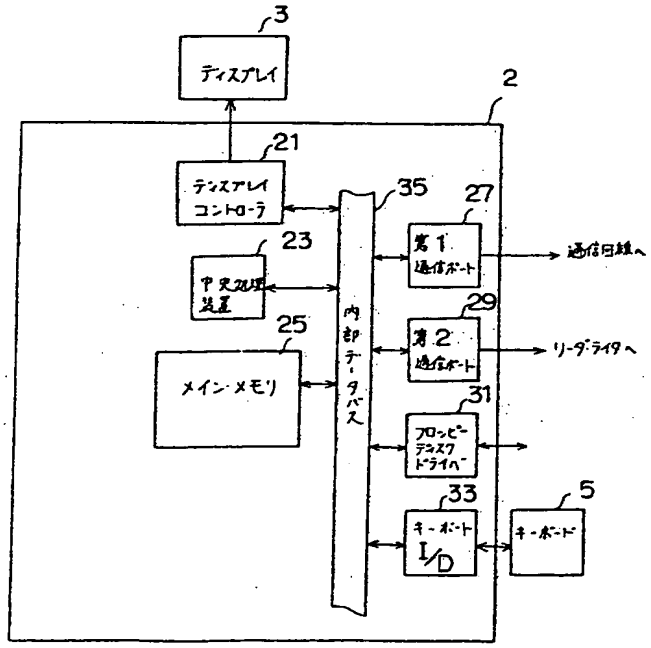
第 1 図



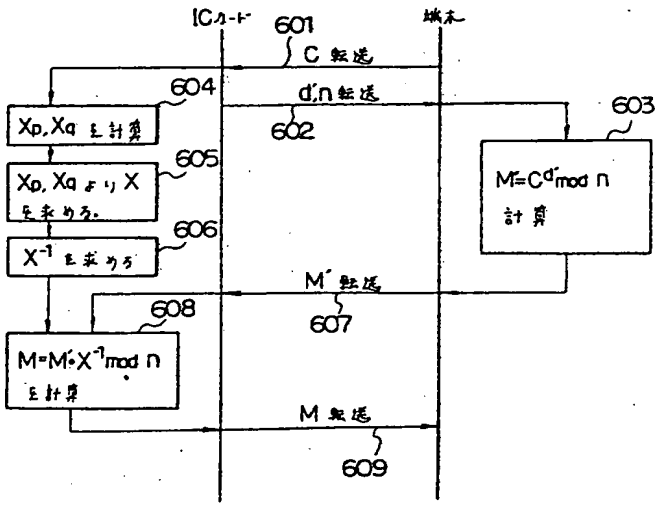
第 2 図



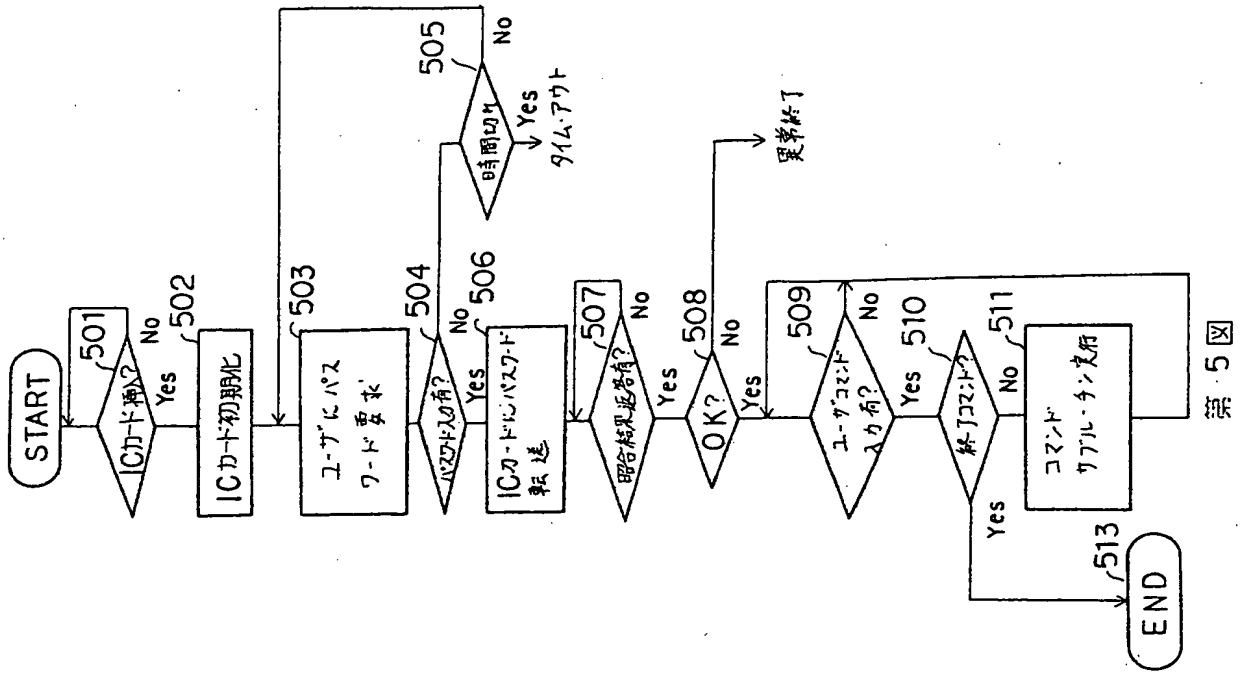
第 3 図



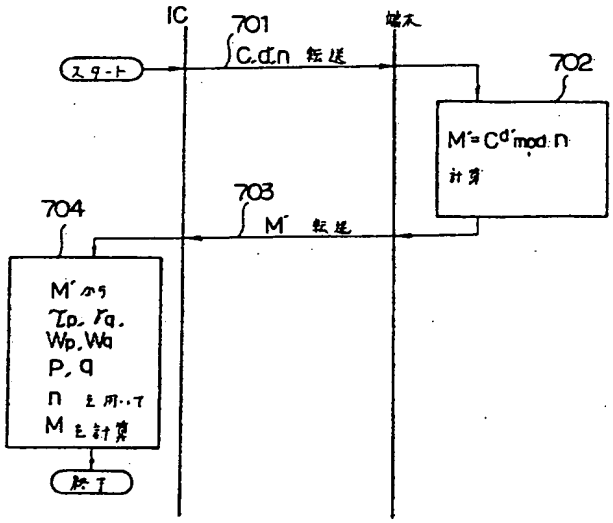
第 4 図



第 6 図


START
501
ICカード挿入?
No
Yes
502
ICカード初期化
503
ユーザにパスワード要求
504
パスワードの有?
No
Yes
505
時間切れ
No
Yes
タイムアウト
506
ICカードにパスワード転送
507
照合結果返答有?
No
Yes
508
OK?
No
Yes
異常終了
509
ユーザコマンド入力有?
No
Yes
510
終了コマンド?
No
Yes
511
コマンドサブルーチン実行
513
END

第 5 図


IC
端末
スタート
701
C, d, n 転送
702
M'=C^d mod n
計算
703
M' 転送
704
M' から
Ip, Iq,
Wp, Wq
P, Q
n を用いて
M を計算
終了

第 7 図